MS-ISAC® EI-ISAC®

Understanding Your Cyber Threat Landscape

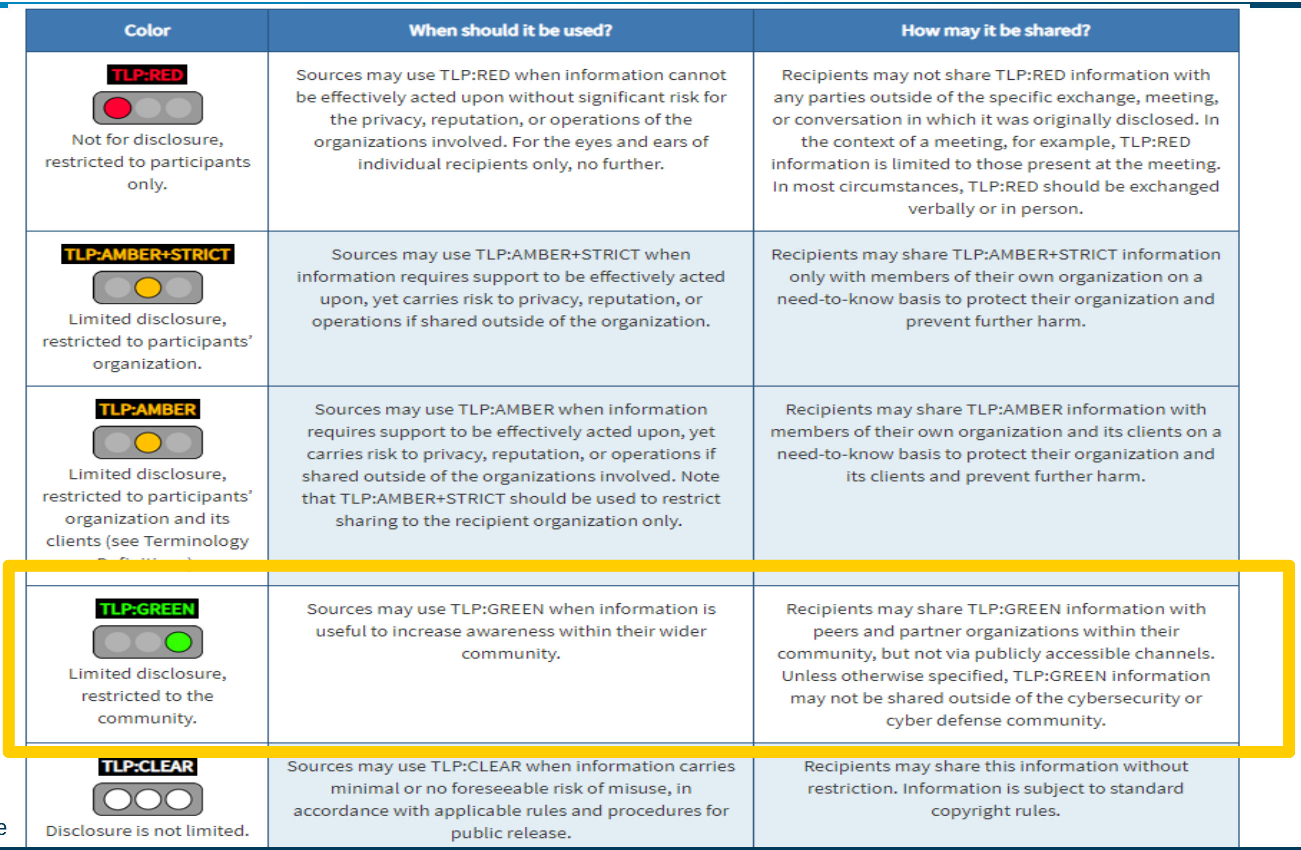
Emily Sochia
Maturity Services Manager

Elijah Cedeno
Regional Engagement Manager

Confidential & Proprietary

TLP Classification

Traffic Light Protocol (TLP)



Color	When should it be used?	How may it be shared?
TLP:RED Not for disclosure, restricted to participants only.	Sources may use TLP:RED when information cannot be effectively acted upon without significant risk for the privacy, reputation, or operations of the organizations involved. For the eyes and ears of individual recipients only, no further.	Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.
TLP:AMBER+STRICT Limited disclosure, restricted to participants' organization.	Sources may use TLP:AMBER+STRICT when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organization.	Recipients may share TLP:AMBER+STRICT information only with members of their own organization on a need-to-know basis to protect their organization and prevent further harm.
TLP:AMBER Limited disclosure, restricted to participants' organization and its clients (see Terminology Definitions).	Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organizations involved. Note that TLP:AMBER+STRICT should be used to restrict sharing to the recipient organization only.	Recipients may share TLP:AMBER information with members of their own organization and its clients on a need-to-know basis to protect their organization and its clients and prevent further harm.
TLP:GREEN Limited disclosure, restricted to the community.	Sources may use TLP:GREEN when information is useful to increase awareness within their wider community.	Recipients may share TLP:GREEN information with peers and partner organizations within their community, but not via publicly accessible channels. Unless otherwise specified, TLP:GREEN information may not be shared outside of the cybersecurity or cyber defense community.
TLP:CLEAR Disclosure is not limited.	Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	Recipients may share this information without restriction. Information is subject to standard copyright rules.

MS-ISAC®
EI-ISAC®

Multi-State Information Sharing & Analysis Center

Who We Serve: State, Local, Tribal, and Territorial Governments

State, Local, Tribal, and Territorial Governments

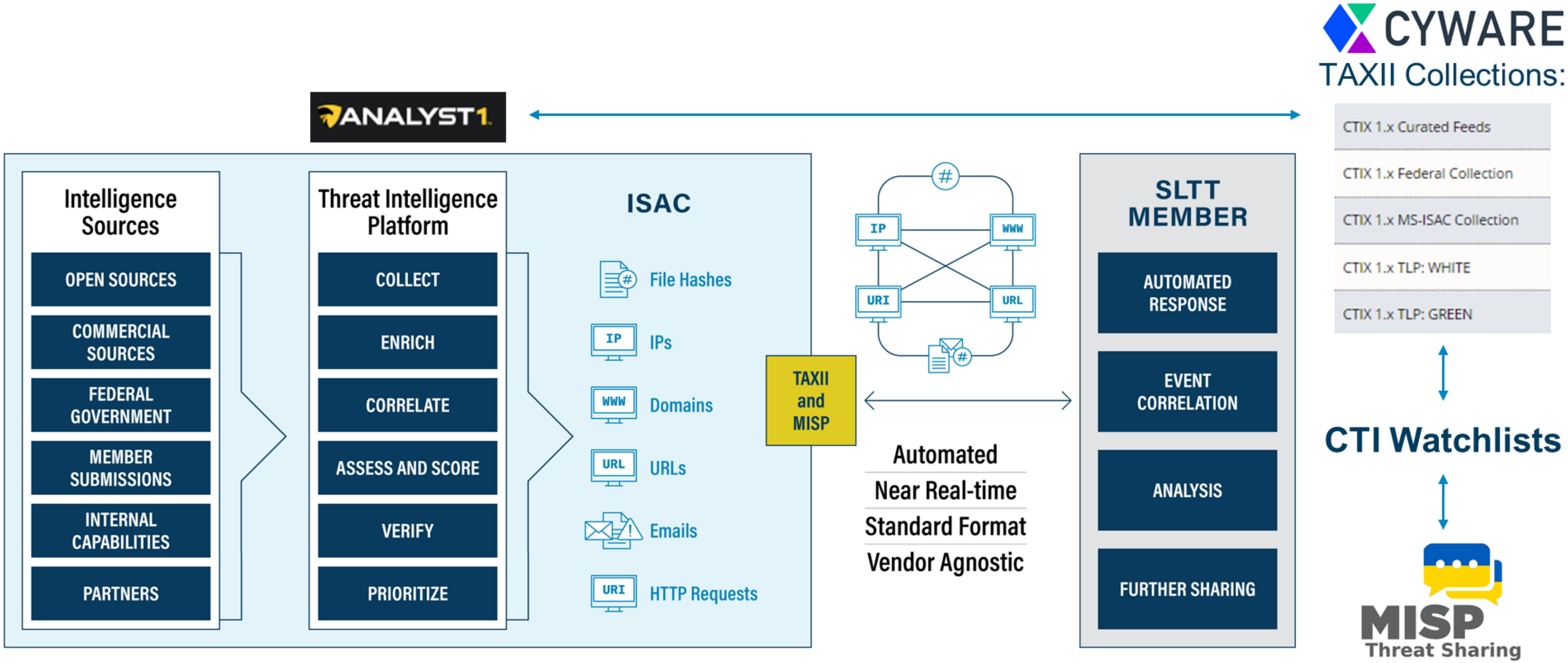
- 50 State Governments
- 15,000 Local Governments!
- 6 Territorial Governments
- 190 Tribal Governments
- 80 DHS-recognized Fusion Centers

Local Governments include

- 1,685 Total Cities
- 1,497 County/Parish/Borough
- 4,443 Public K-12 Schools
- 675 Town/Township/Village

Processing & Analysis

Indicator Sharing Program



ANALYST1

CYWARE

TAXII Collections:

- CTIX 1.x Curated Feeds
- CTIX 1.x Federal Collection
- CTIX 1.x MS-ISAC Collection
- CTIX 1.x TLP: WHITE
- CTIX 1.x TLP: GREEN

CTI Watchlists

MISP Threat Sharing

Intelligence Sources

- OPEN SOURCES
- COMMERCIAL SOURCES
- FEDERAL GOVERNMENT
- MEMBER SUBMISSIONS
- INTERNAL CAPABILITIES
- PARTNERS

Threat Intelligence Platform

- COLLECT
- ENRICH
- CORRELATE
- ASSESS AND SCORE
- VERIFY
- PRIORITIZE

ISAC

- File Hashes
- IPs
- Domains
- URLs
- Emails
- HTTP Requests

TAXII and MISP

Automated

Near Real-time

Standard Format

Vendor Agnostic

SLTT MEMBER

- AUTOMATED RESPONSE
- EVENT CORRELATION
- ANALYSIS
- FURTHER SHARING

Unique Threats to Local Governments

- **Overseeing critical community resources and services**
- **Often under-resourced and lacking sufficient training**
  - Includes important functions like timely patching, controls, threat intelligence
  - Appeals to CTAs
- **Budgets and cyber insurance coverage publicly available**
- **Emsisoft: At least 31 ransomware incidents impacting sector this year**

MS-ISAC®
EI-ISAC®

Social Engineering

Exploiting the End User

- **Phishing:** Cyber threat actors (CTAs) masquerade as legitimate entities to trick users into opening attachments, clicking links, or providing sensitive information.
- Often meant to provoke sense of urgency
- Phishing themes and lures include ongoing crises (e.g. hurricanes, COVID-19, etc..) or seasonal events (e.g. Tax Season)

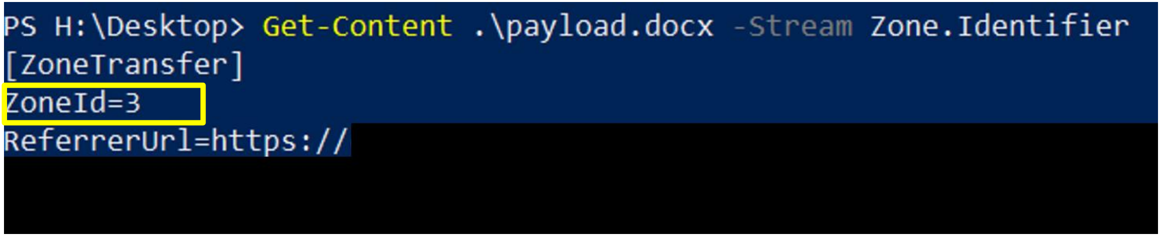
Business email compromise (BEC):

- A type of phishing scam where attacker impersonates or compromises an executive's email account to manipulate the target into initiating a wire transfer or to giving away sensitive information.

Microsoft Blocking Macros

Cyber actors pivot tactics

- Microsoft announced in February that macros from the internet will be blocked by default in Office applications
- Office documents originating from an email attachment or from the internet have a Mark of the Web (MOTW)
- Blocking macros will give increased security for files originating from the internet

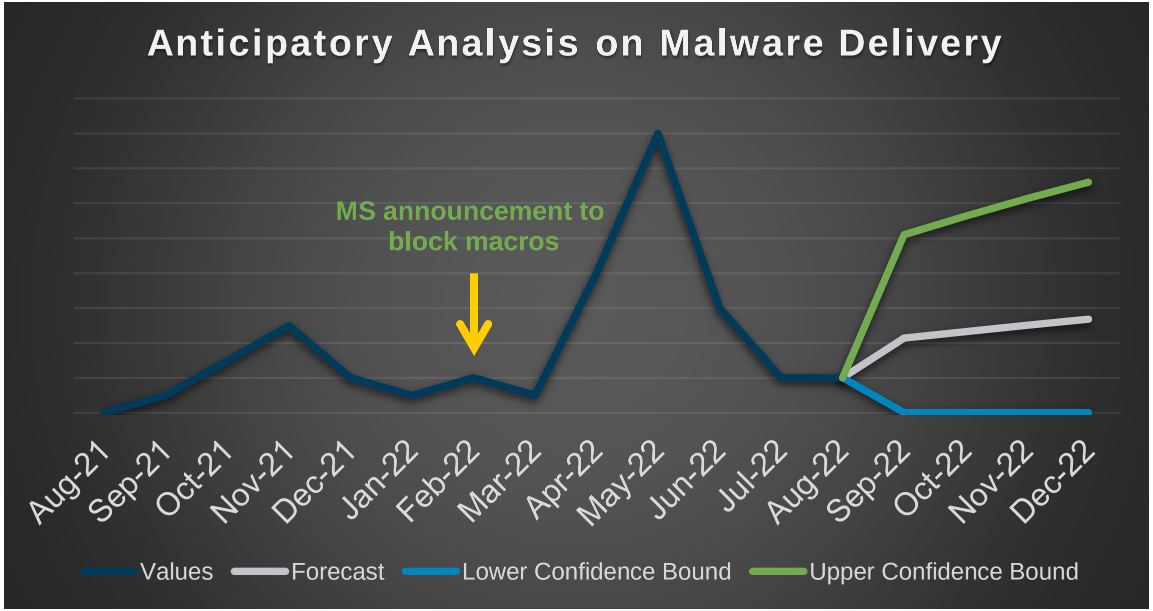


```
PS H:\Desktop> Get-Content .\payload.docx -Stream Zone.Identifier
[ZoneTransfer]
ZoneId=3
ReferrerUrl=https://[redacted]
```

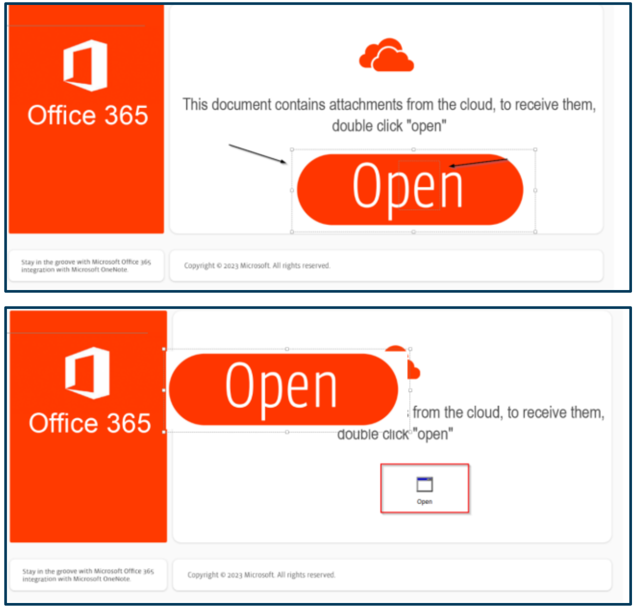
0 = Local Machine
1 = Intranet
2 = Trusted
3 = Internet
4 = Untrusted

SLTT Threat Landscape

MOTW: Forecasts & Methods



.LNK File Delivery Trend



This document contains attachments from the cloud, to receive them, double click "open"

Stay in the groove with Microsoft Office 365 integration with Microsoft OneNote.

Copyright © 2023 Microsoft. All rights reserved.

from the cloud, to receive them, double click "open"

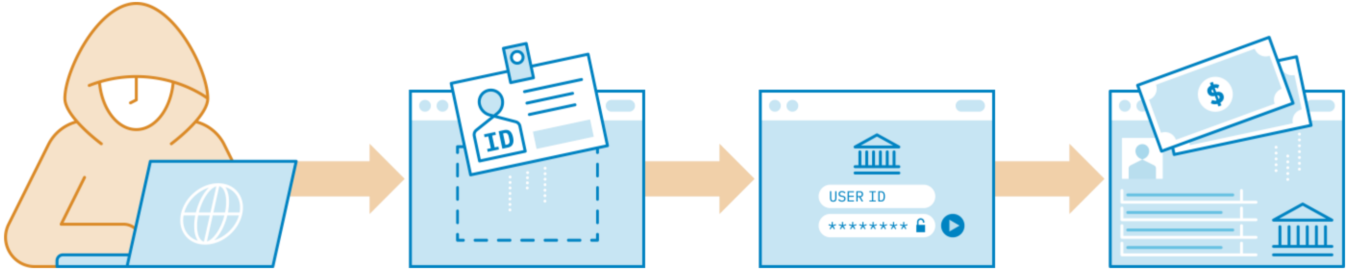
Stay in the groove with Microsoft Office 365 integration with Microsoft OneNote.

Copyright © 2023 Microsoft. All rights reserved.

OneNote Delivery Example

Breached Credential Service

- Compromised Credentials provide an easy initial access vector for attackers
- Once initial access is established, attackers can escalate privileges and move laterally
- Credential reuse is unfortunately very common and attackers may attempt to use a breached Spotify or Twitter password to compromise a more valuable account

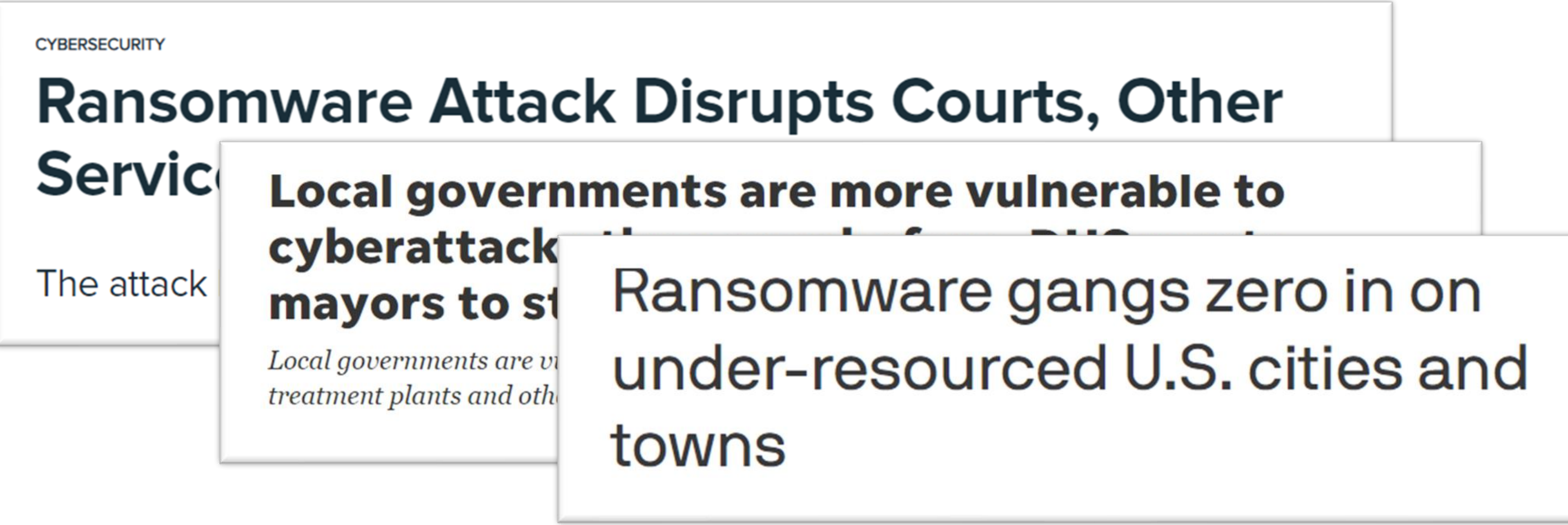


MS-ISAC®
EI-ISAC®

Breached Credential Service

- CTI has begun issuing notifications to our members when credentials from their domains are breached
- We scrape data from the web for compromised credentials
- Tailor our search for SLTT domains
- Notifications are sent to those members on a weekly cadence

Ransomware Making Headlines



CYBERSECURITY

Ransomware Attack Disrupts Courts, Other Servic

The attack

Local governments are more vulnerable to cyberattack

mayors to st

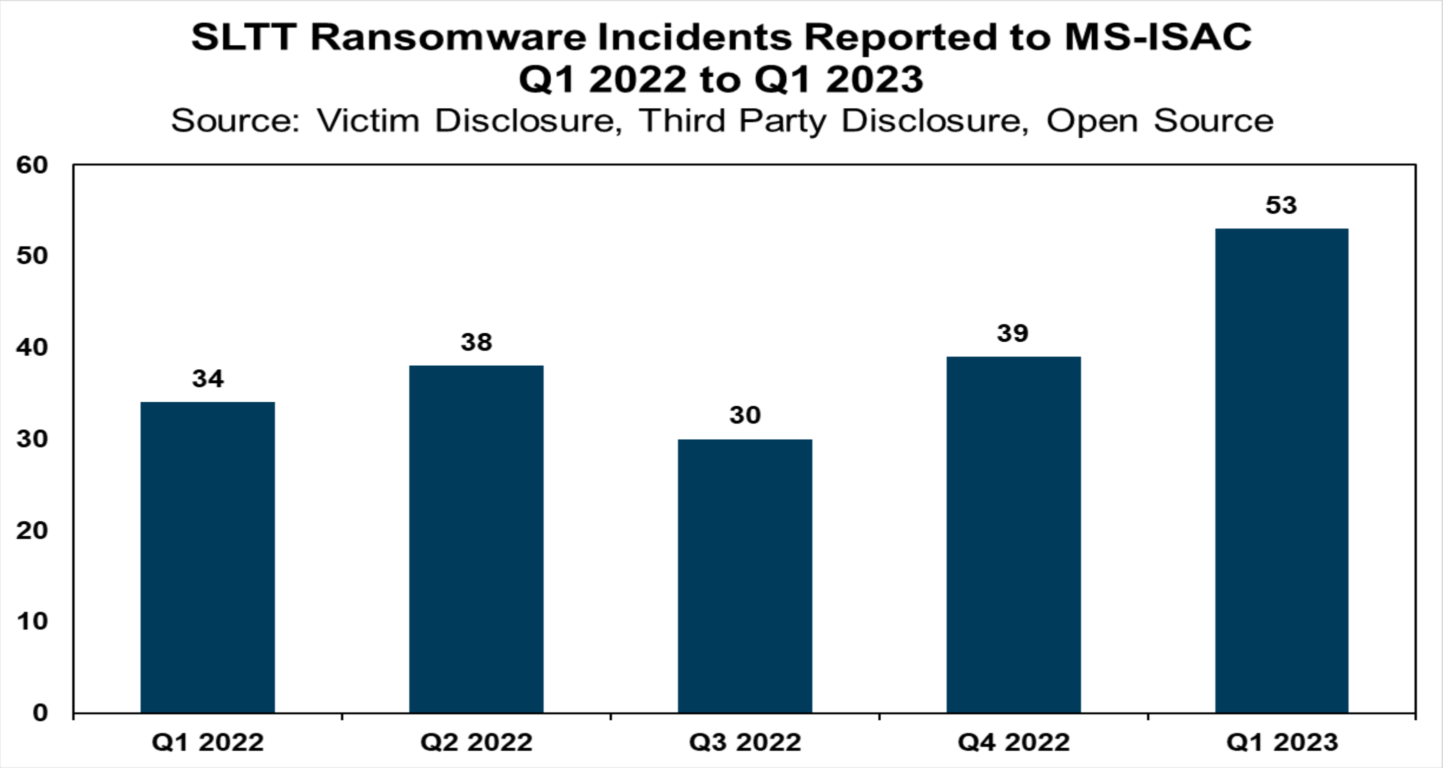
Local governments are vu

treatment plants and oth

Ransomware gangs zero in on under-resourced U.S. cities and towns

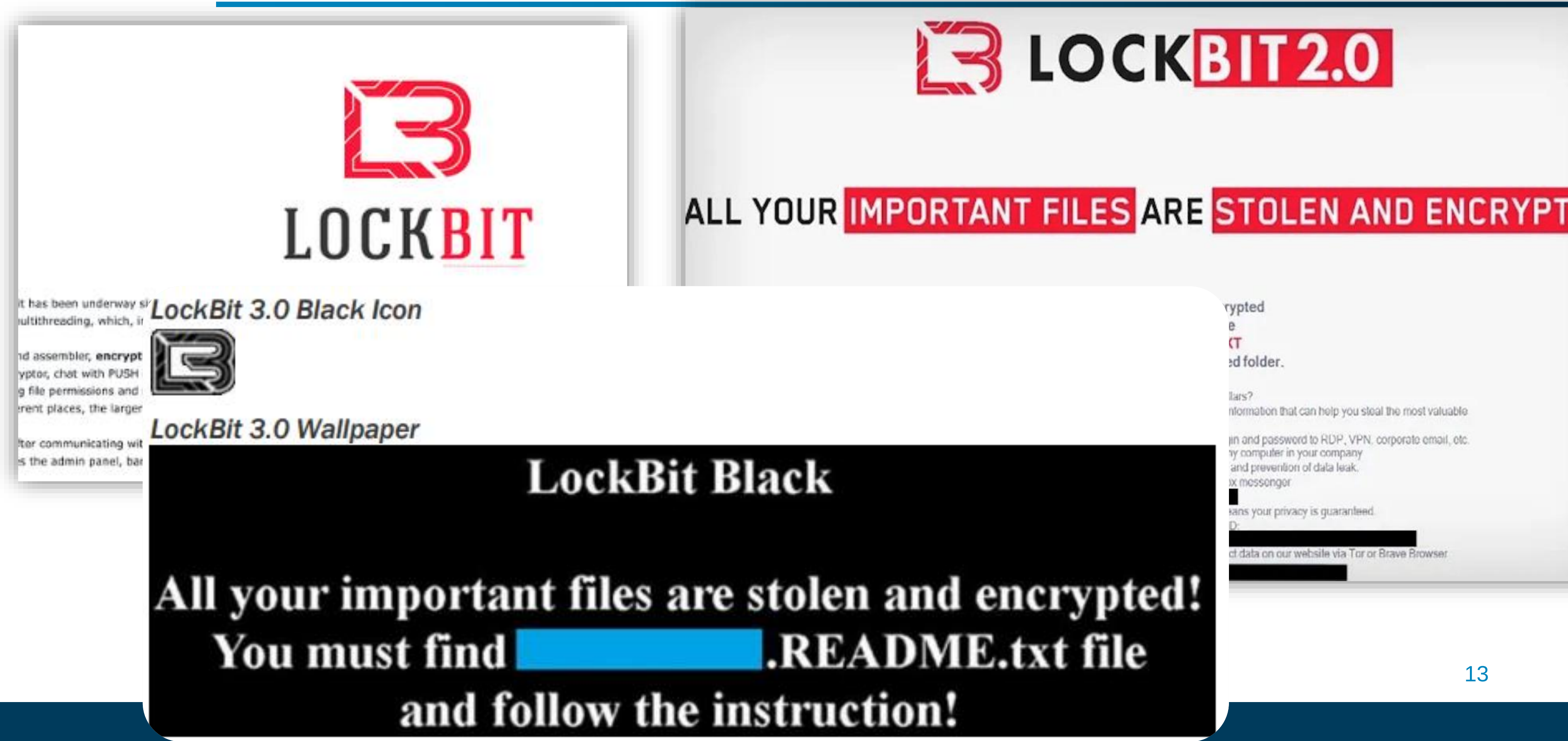
SLTT Threat Landscape

Ransomware Trends



Lockbit Ransomware

Versions 1.0, 2.0 and Black



it has been underway si
ultithreading, which, i

nd assembler, **encrypt**
yptor, chat with PUSH
g file permissions and
erent places, the larger

ter communicating wit
s the admin panel, ba

ALL YOUR IMPORTANT FILES ARE STOLEN AND ENCRYPT

rypted
e
XT
ed folder.

llars?
nformation that can help you steal the most valuable

gin and password to RDP, VPN, corporate email, etc.
ny computer in your company
and prevention of data leak.
x messenger
[redacted]
ans your privacy is guaranteed
D:
[redacted]
ct data on our website via Tor or Brave Browser
[redacted]

LockBit 3.0 Black Icon

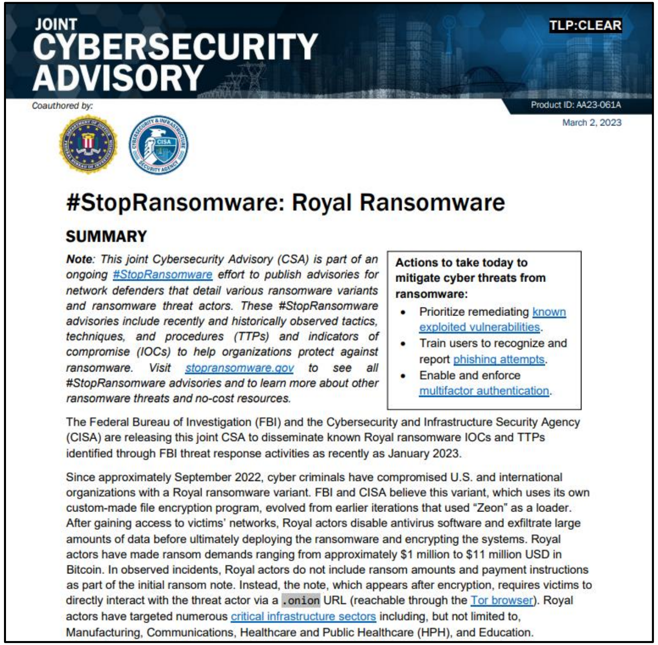
LockBit 3.0 Wallpaper

LockBit Black

All your important files are stolen and encrypted!
You must find [redacted].README.txt file
and follow the instruction!

Cyber Threat Intelligence (CTI)

MS-ISAC



JOINT CYBERSECURITY ADVISORY

TLP:CLEAR

Coauthored by:

Product ID: AA23-061A

March 2, 2023

#StopRansomware: Royal Ransomware

SUMMARY

Note: This joint Cybersecurity Advisory (CSA) is part of an ongoing #StopRansomware effort to publish advisories for network defenders that detail various ransomware variants and ransomware threat actors. These #StopRansomware advisories include recently and historically observed tactics, techniques, and procedures (TTPs) and indicators of compromise (IOCs) to help organizations protect against ransomware. Visit stopransomware.gov to see all #StopRansomware advisories and to learn more about other ransomware threats and no-cost resources.

Actions to take today to mitigate cyber threats from ransomware:

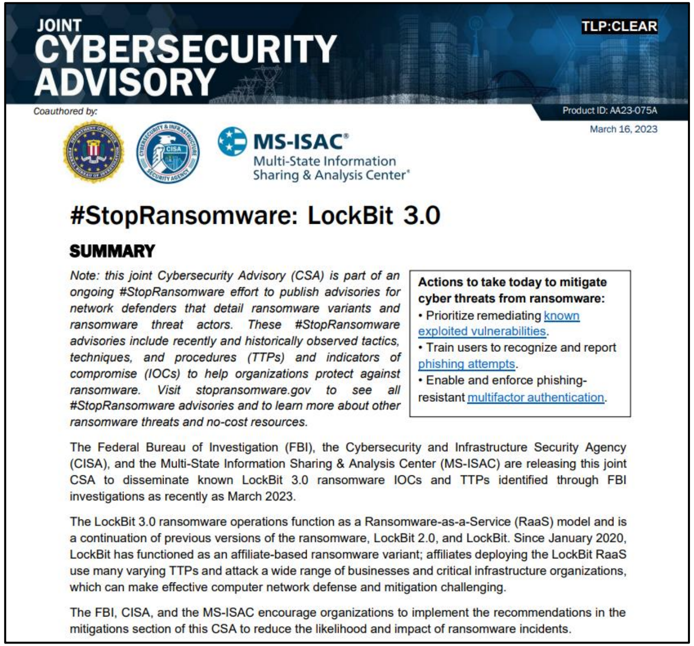
- Prioritize remediating known exploited vulnerabilities.
- Train users to recognize and report phishing attempts.
- Enable and enforce multifactor authentication.

The Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) are releasing this joint CSA to disseminate known Royal ransomware IOCs and TTPs identified through FBI threat response activities as recently as January 2023.

Since approximately September 2022, cyber criminals have compromised U.S. and international organizations with a Royal ransomware variant. FBI and CISA believe this variant, which uses its own custom-made file encryption program, evolved from earlier iterations that used "Zeon" as a loader. After gaining access to victims' networks, Royal actors disable antivirus software and exfiltrate large amounts of data before ultimately deploying the ransomware and encrypting the systems. Royal actors have made ransom demands ranging from approximately $1 million to $11 million USD in Bitcoin. In observed incidents, Royal actors do not include ransom amounts and payment instructions as part of the initial ransom note. Instead, the note, which appears after encryption, requires victims to directly interact with the threat actor via a `.onion` URL (reachable through the Tor browser). Royal actors have targeted numerous critical infrastructure sectors including, but not limited to, Manufacturing, Communications, Healthcare and Public Healthcare (HPH), and Education.

March 2, 2023

https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-061a



JOINT CYBERSECURITY ADVISORY

TLP:CLEAR

Coauthored by:

Product ID: AA23-075A

March 16, 2023

MS-ISAC® Multi-State Information Sharing & Analysis Center®

#StopRansomware: LockBit 3.0

SUMMARY

Note: this joint Cybersecurity Advisory (CSA) is part of an ongoing #StopRansomware effort to publish advisories for network defenders that detail ransomware variants and ransomware threat actors. These #StopRansomware advisories include recently and historically observed tactics, techniques, and procedures (TTPs) and indicators of compromise (IOCs) to help organizations protect against ransomware. Visit stopransomware.gov to see all #StopRansomware advisories and to learn more about other ransomware threats and no-cost resources.

Actions to take today to mitigate cyber threats from ransomware:

- Prioritize remediating known exploited vulnerabilities.
- Train users to recognize and report phishing attempts.
- Enable and enforce phishing-resistant multifactor authentication.

The Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), and the Multi-State Information Sharing & Analysis Center (MS-ISAC) are releasing this joint CSA to disseminate known LockBit 3.0 ransomware IOCs and TTPs identified through FBI investigations as recently as March 2023.

The LockBit 3.0 ransomware operations function as a Ransomware-as-a-Service (RaaS) model and is a continuation of previous versions of the ransomware, LockBit 2.0, and LockBit. Since January 2020, LockBit has functioned as an affiliate-based ransomware variant; affiliates deploying the LockBit RaaS use many varying TTPs and attack a wide range of businesses and critical infrastructure organizations, which can make effective computer network defense and mitigation challenging.

The FBI, CISA, and the MS-ISAC encourage organizations to implement the recommendations in the mitigations section of this CSA to reduce the likelihood and impact of ransomware incidents.

March 16, 2023

https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-075a

MS-ISAC®
Multi-State Information
Sharing & Analysis Center®

Elections
Infrastructure
ISAC®

NCSR Key Findings and Recommendations

Nationwide Cybersecurity Review (NCSR)

https://www.cisecurity.org/ms-isac/services/ncsr

A no-cost, anonymous, annual self-assessment based on NIST CSF

(open October – February)

Requirement for the Homeland Security Grant Program (HSGP) and the State and Local Cybersecurity Grant Program (SLCGP)

NATIONWIDE CYBERSECURITY REVIEW

Organization specific metrics; Reporting templates and resources to help with prioritization

NCSR information & registration:

MS-ISAC®

NIST Framework & Resource Mapping

Identify

- Nationwide Cybersecurity Review (NCSR)
- CIS Controls
- NIST Cybersecurity Framework Policy Template Guide
- Real-Time Indicator Feeds
- CISA Supply Chain Resource Library [1]

Protect

- CIS Benchmarks
- CIS SecureSuite
- MS-ISAC Tabletop Exercises (TTX)
- MS-ISAC Toolkit

Detect

- 24x7x365 MS-ISAC Security Operations Center
- Passive IP & Domain Monitoring
- Malicious Domain Blocking & Reporting (MDBR)
- CISA Cyber Hygiene Program (CYHY)[1]

Respond

- 24x7x365 MS-ISAC Cyber Incident Response Team (CIRT)
- MS-ISAC Tabletop Exercises (TTX)
- Homeland Security Information Network (HSIN)[1]

Recover

- 24x7x365 MS-ISAC Cyber Incident Response Team (CIRT)
- NIST Cybersecurity Framework Policy Template Guide
- MS-ISAC Tabletop Exercises (TTX)
- Homeland Security Information Network (HSIN)[1]

2022 General NCSR Findings

*Preliminary Anonymized Findings Across all 2022 Participants

- **Security Framework Usage**
  - Entities that stated they utilize a security framework, such as the CIS Controls, NIST CSF, and ISO 27000 series, scored 58% higher than organizations that did not.
- **2022 High Performing Areas**
  - PR.AC
  - PR.AT
  - RC.RP
- **2022 Deficient Performing Areas**
  - ID.RM
  - RS.IM, RC.IM

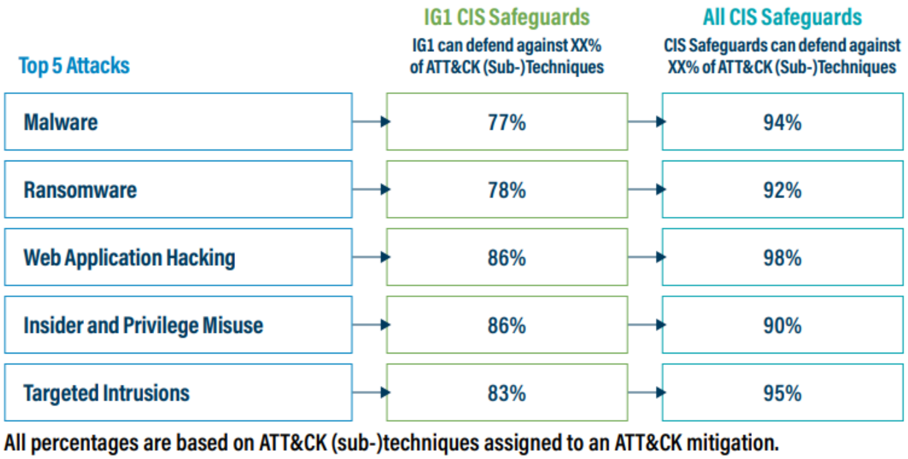
CIS Controls

Preparation is Key

- **CIS Critical Security Controls**
  - Provide a prioritized set of actions to protect your organization and data from known cyber-attack vectors.
  - https://www.cisecurity.org/controls/

- **CIS Community Defense Model 2.0**
  - How effective are the CIS Controls against the most prevalent types of attacks?
  - https://www.cisecurity.org/insights/white-papers/cis-community-defense-model-2-0

CIS Controls



Top 5 Attacks	IG1 CIS Safeguards IG1 can defend against XX% of ATT&CK (Sub-)Techniques	All CIS Safeguards CIS Safeguards can defend against XX% of ATT&CK (Sub-)Techniques
Malware	77%	94%
Ransomware	78%	92%
Web Application Hacking	86%	98%
Insider and Privilege Misuse	86%	90%
Targeted Intrusions	83%	95%

All percentages are based on ATT&CK (sub-)techniques assigned to an ATT&CK mitigation.

CISA Guidance

Preparation is Key

- **CISA Stop Ransomware Webpage**
  - The U.S. Government's official one-stop location for resources to tackle ransomware more effectively.
  - https://www.cisa.gov/stopransomware
- **CISA/MS-ISAC Joint Ransomware Guide**
  - Best practices and incident response guidance
  - https://www.cisa.gov/stopransomware/ransomware-guide

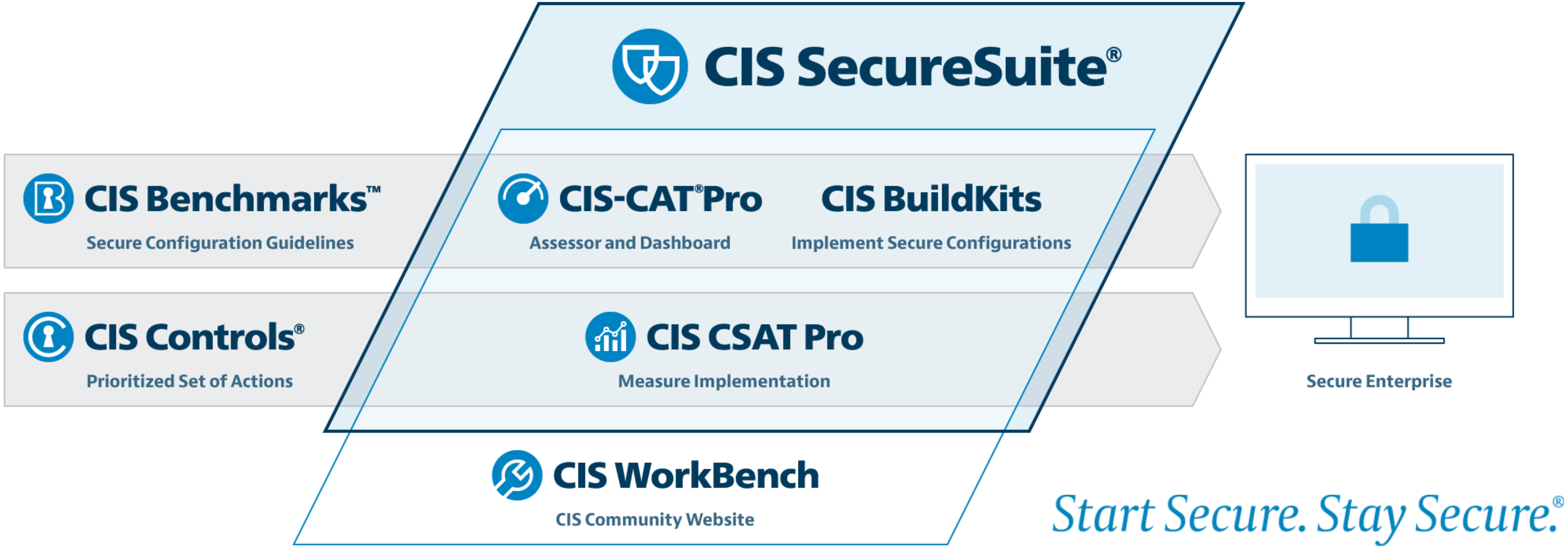
RANSOMWARE GUIDE

SEPTEMBER 2020

MS-ISAC®
Multi-State Information Sharing & Analysis Center®

CIS SecureSuite®

FreeSecureSuite@cisecurity.org



https://www.cisecurity.org/cis-securesuite/member-webinars

Confidential & Proprietary

TLP:GREEN

MS-ISAC®

Security Operations Center

24x7x365

Support

Network Monitoring Services
+
Research and Analysis

Analysis & Monitoring

Threats, Vulnerabilities
+
Attacks

Reporting

Cyber Alerts & Advisories

Web Defacements

Account Compromises

To report an incident or request assistance:

Phone: 1-866-787-4722

Email: soc@cisecurity.org

Confidential & Proprietary

TLP:GREEN

MS-ISAC®

Cyber Incident Response Team (CIRT)

- Incident Response
- Malware Analysis
- Log Analysis

To report an incident or request assistance:

Phone: 1-866-787-4722

Email: soc@cisecurity.org

MS-ISAC®

Multi-State Information Sharing & Analysis Center®

Thank You!

Contact Us

Security Operations Center

24/7 Phone Number

1-866-787-4722

soc@msisac.org

intel@cisecurity.org

info@msisac.org